A

Synopsis

On

Security of Data Sharing in Cloud Computing

For Registration

Of

DOCTOR OF PHILOSOPHY

In

Computer Science and Applications

Submitted By:
Sameer Anand
Roll. No. 05

Under the Supervision of :
Dr. Harish Rohil, Associate Prof.
Dept. of Computer Sc. &Appls.
C.D.L.U, Sirsa

Department of Computer Science & Applications

Chaudhary Devi Lal University, Sirsa-125055 (India)

2017-18

INDEX

Title	Page No.
1. Introduction	3
2. Cloud Computing	4
3. Data Sharing in Cloud Computing	6
4. Cryptography	7
4.1 Symmetric Cryptography	7
4.2 Asymmetric Cryptography	8
4.2.1 Elliptic curve cryptography	8
4.2.2 Diffie-Hellman algorithm	9
4.2.3 Prime Factorization in cryptography	11
5 Review of Existing Approaches	11
6 Research Methodology	15
6.1 Problem Statement	15
6.2 Research objectives	15
6.3 Research Methodology	16
References	17

Security of Data Sharing in Cloud Computing

1 Introduction

Cloud computing system is the novel version of utility computing that has substituted its area at different data centers. The consumers have wide-ranging access to information technology capabilities and facilities which is delivered through the Internet and has carried a marvelous variation inthe processes of IT industries. It also helped the IT industries with less infrastructure investment besides maintenance [1].

It is becoming popular as virtualization power, distributed computing with server cluster and rise in the availability of broadband internet assessing is increasing. The IT world is looking forward to the services delivered and consequently enhancing the growth of cloud computing [2].

Using the cost-effectiveness enhancements in the computational technology and large-scale networks, sharing information through theothers turn out to be congruently more useful. Moreover, digital resources are more simply acquired through cloud computing in addition to storage. Meanwhile, cloud data sharing needs off-premises infrastructure that particular organizations mutually held, remote storage is someway intimidating confidentiality of data owners. Consequently, enforcing the security of personal [3].

Computer security is critical in almost any technology-driven industry that functions on computer systems. The essential objective in security is to offer a cryptographic system that is computationally infeasible for attackers to achieve the right to use to the system. When designing a computer system, there are numerous aspects to be taken into concern, among that one of the main factor is security, which proves to be very significant. For Instance, the problem of integer factorization is a method utilized in RSA. The discrete logarithm is preferred in DH Key Exchange, Digital Signature Algorithm, Elliptic Curve Cryptography and so on. These primitives are founded on hard AI problems.

The problem of instantaneously attaining fine-grainedness, high efficiency on the data owner's side, and standard data confidentiality of cloud data sharing remain vague. There is no constituency among the data synchronization besides data storage. Essential to enhance the system security mechanism.

The proposed Decisional Bilinear Diffie-Factorial Prime Elliptic Curve Hellman Cryptographic Data Sharing in cloud computing (DBECC) is to Secure the sharing of data in cloud computing. Moreover, it is also to focus on all the type of Attacks in the area of Cloud Computing. It also used to prevent the data from Brute Force Attack, Dictionary Attack, SQL Injection Attack, collusion Attacks, and Side Channel Attacks.

2. Cloud Computing

Cloud is a computing technology which is based on the internet, where shared resources such as software, platform, storage, and information are offered to customers on demand. It is a computing platform for sharing resources that consist of infrastructures, software, applications, and business procedures. It is a virtual pool of computing resources. It delivers computing resources in the pool for users over the internet. It is also a developing computing model aims to share storage, computation, and services transparently between the massive users. Existing Cloud computing systems posses severe drawback in protecting users' data confidentiality.

Meanwhile, users' sensitive data is offered in unencrypted forms to remote machines owned and functioned through third party service providers, the risks of unauthorized disclosure of the users' sensitive data through service providers might be quite high. There are numerous methods intended for protecting users' data from external attackers. Cloud computing systems offer different internet-based data storage and services. Due to its several major benefits, containing cost efficiency in addition to high scalability and flexibility, it is gaining substantial momentum newly as a novel standard of distributed computing for

different applications, particularly for the applications of business together with the rapid development of the Internet.

The term "Cloud" in Cloud computing is the communication network, or a networkis Combined with the computing infrastructure. It is accessed using a network which provides software, hardware, processing power, etc. to the user when demand is generated. It is a virtual pool of computing resources which provides the pool to users through the internet.

Cloud Computing [4] provides various services to the user by creating a group of clusters and grids of computers. The main goal behind this is to provide services in a virtualized manner to reduce the burden of the user to maintain everything by itself. It similarly states to the web-based computing that offers devices using a shared pool of resources, information or else software on demand and also by pay-per-use. Instead of possessing local servers or own devices to manage applications, people use sharing computing resources model of Cloud.

It also provides an environment in which user can have its virtual infrastructure using which they can perform tasks without depending on a geographical boundary. Because of the flexible environment and cheaper cost, people are attracted to the use of Cloud services that may be related to Platform, software orinfrastructure. Based on the usage of Cloud, there are three deployment models: Public Cloud, Private Cloud, and Hybrid Cloud. Cloud computing provides a numerous advantage to its users, but on the other side, it also suffers from lots of issues like Integrity or Storage Correctness, Availability, Confidentiality and more. These issues make the adaption of cloud environment somewhat difficult for the users.

3. Data sharing in Cloud Computing

There are numerous security problems and challenges in cloud computing technology. The security problems in cloud computing are specified in [5]. It is necessary for the network on the cloud which is responsible for interconnection among the systems to be safe and secure. it also has virtualization patterns which give rise to many security problems. Thus to map virtual machines into physical machines, high security is required. The data securities include encryption of the data and ensure relevant policies needed to carry out data sharing. The allocation of resources and the memory managing algorithms should be highly protected and safe. One of the major problems in cloud computing is that it implicitly consists of the business-critical data and complex processes and also outsources sensitive data securely. The data stored on a cloud service is the responsibility of the cloud provider who controls and protects those data. When the data is organized on the cloud through IaaS or PaaS, then the complete control is possessed by the cloud provider.

For this reason, a trustworthy relationship among the cloud users and the Cloud Service Providers (CSPs)is required for which several types of research are carried out. The security threats faced by most of the computing systems are all also faced by cloud computing technology. One of the major issuesis Protecting the confidentiality and sensitive files are outsourced,and nowadays this is applicable in mobiles for the misusing of data or violating the integrity of data. The processed files present in cloud storage are kept away from illegal users by utilizing the attribute-based encryption for controlling the admission of the files being encrypted by the Data Owners.

4. Cryptography

Cryptography can be an art,or it is the science of encrypting and decrypting the communication to be protected when transferring over an insecure and untrusted network; it can be attained by designing cryptographic techniques. On the other side, cryptanalysis is the art. Or, it is the science of studying and analyzing cryptographic techniques to break them. It is clear that cryptography and cryptanalysis are interconnected, Mustafa. In 1976, cryptography underwent to a singular development after D-H present a paper entitled with "new directions in cryptography" [6] that shows the public key concept and the different methods of key exchange protocol.

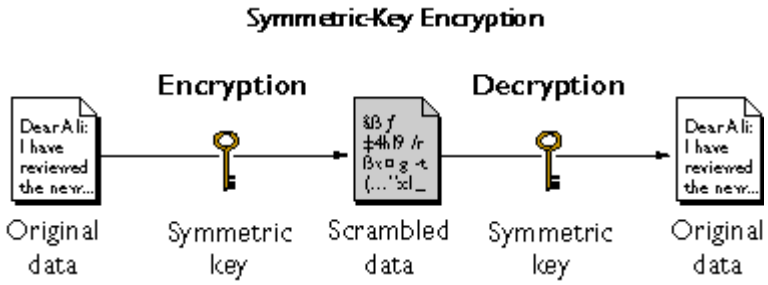
Cryptography algorithms differentiate into two main categories:

(i) Symmetric cryptography

(ii) Asymmetric cryptography

4.1 Symmetric cryptography

It has only one key to encrypt or decrypt the information over insure channel.



Secured cloud is an important research issue as it deals with a variety of customers, and various devices and metrics. A smaller size of security keys will be preferred as the clouds are accessed by many handheld devices. So the important point which comes to mind is the security with small key size [7]. Cryptography has become one of the major sciences in the present era. The significance of cryptography derives from the intensive digital communications that we regularly perform on the internet in addition to further

communication channels. Symmetric Cryptography also provides a degree of authentication because data encrypted with one symmetric key cannot be decrypted with any other symmetric key.Therefore as long as symmetric key is kept secret by two parties using it to encrypt communications,each party can be sure that it is communicating with the other as long as the decrypted messages conitune to make sence.In a symmetric key,you can exchange the key with another trusted participant.usually you produce a key for each pair of participants.

Asymmetric cryptography

Asymmetric cryptography is of 3 Types-

1) Elliptic curve Cryptography.
2) Diffie-Hellman Cryptography.
3) Prime Factorization in Cryptography.

4.2.1 Elliptic curve cryptography:-

ECCcomes under the category of asymmetric cryptography because it uses one key for encryption and another key for decryption. It is secured for key- exchange, authentication, and non-repudiation. It is well-defined as the method concerning PKC based on the mathematical structure of elliptic curves over finite fields. The advantage of elliptical curves is they require very small keys but still ensure maximum security [9]. There are different tasks which apply to the elliptical curves in which digital signatures and encryption are to name a few. The security of ECC will vary based on the capability to compute a point multiplication. The size of the elliptic curves states the complexity of the problem. An elliptic curve is a plane curve over a finite field which contains the points satisfying an equation:

$$y^2 = x^3 + ax + b$$

The coordinates from the beyond equationis needed to be selected from a finite field of characters which are not equivalent to 2 or 3 else the equation of a curve that may be very

difficult. In ECC, the field is well-defined usingp in a prime case in addition to a pair of m and f in binary case. The constants in the curve are ‘a’ and ‘b’ which are used in defining the equation. There are several integer factorization algorithms which have the vast applications in the area of cryptography likeLenstra curve factorization [10].

4.2.2 Diffie-Hellman Algorithm

Diffie-Hellman (D-H) is also comes under the asymmetric cryptography. It is a significant technique of exchanging the keys amongst two parties. It is the most basic examples of key exchange applied inside the cryptography field. That shared secret key can be utilized to encode the information using a symmetric key cipher. The D-H algorithm is utilized to create the public key. The symmetric public key algorithm is interchanging the secret key amongst two users over an insecure channel without any previous knowledge. The D-H functionality is restricted to key exchange only. D-H key exchange algorithm cannot be utilized for encryption as well as decryption, and it doesn’t offer any verification amongst two parties. D-H algorithm major difficulty is that it is susceptible to man-in-the-middle attack [11].

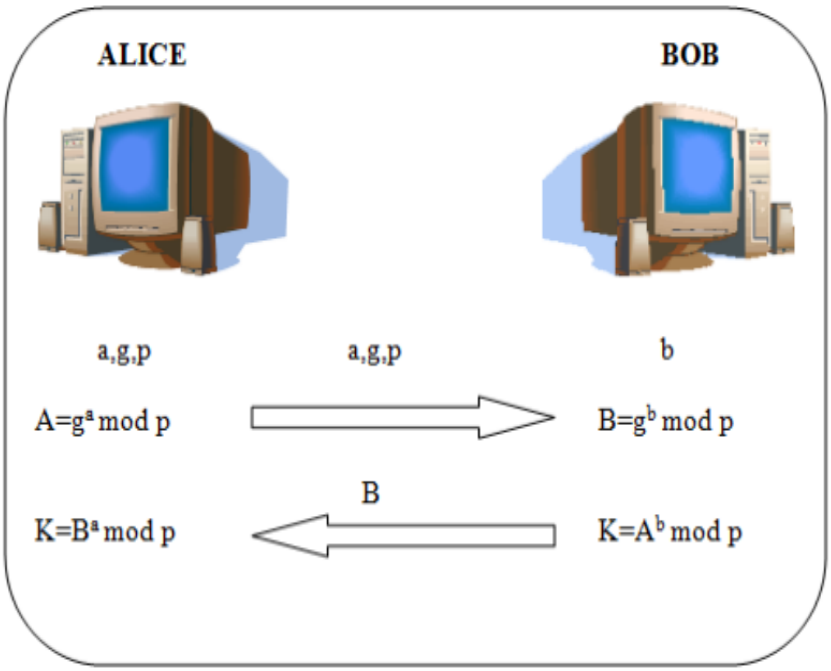


Figure 1 Basic Diagram of D-H Algorithm

The flow chart of the classical D-H algorithm is given in Figure 2. It will describe how classical D-H algorithm will work. In the present algorithm, time complexity and analysis will be measured as well as a D-H key will be used for encryption and decryption using the proposed algorithm. The RSA and D-H key exchange protocol is public key encryption algorithms that are used for commercial purposes [12]. The minimum needed key length for encryption and decryptionsystems is 128 bits, although both algorithms use 1024-bit keys. Both algorithms were introduced in 1970 and had to be cracked.

The nature of the D-H key exchange is suffering from the man-in-the-middle (MITM) attacks since it doesn't provide authentication for both the parties engaged in the interchange process. Moreover, MITM create a key pair with Alice and Bob and get all the messages between two parties, whereas Alice and Bob think they're both communicating each other. Due to a MITM attack, D-H key exchange procedure does not provide authentication.

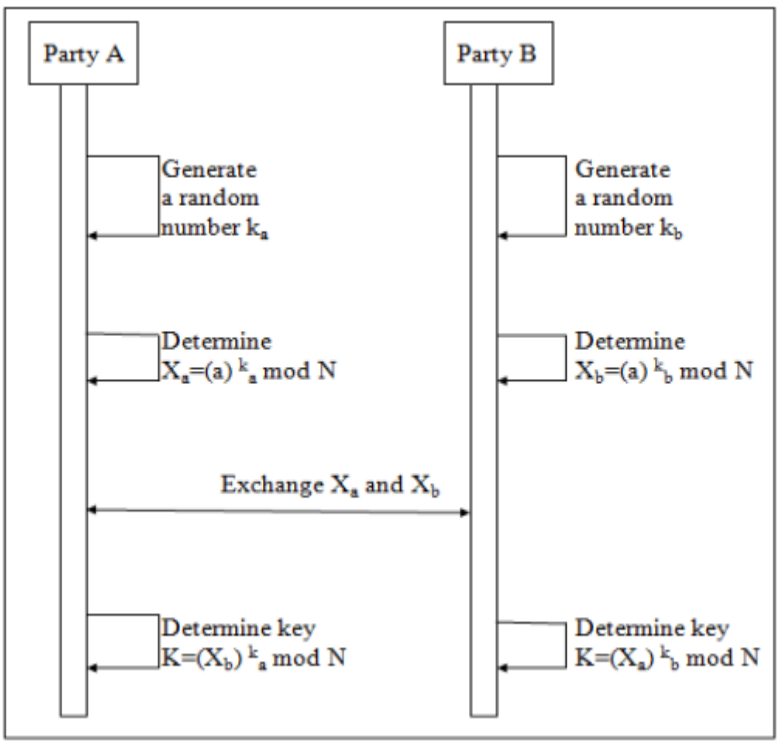

Party A
Party B
Generate a random number k_a
Generate a random number k_b
Determine $X_a=(a)^{k_a} \bmod N$
Determine $X_b=(a)^{k_b} \bmod N$
Exchange X_a and X_b
Determine key $K=(X_b)^{k_a} \bmod N$
Determine key $K=(X_a)^{k_b} \bmod N$

Figure 2 Flow chart of the Diffie-Hellman algorithm [2]

4.2.3 Prime Factorization in cryptography

In number theory, integer factorization or prime factorization is the decomposition of a compositenumber into smaller non-trivial divisors, which when multiplied together equals the original integer. It is also known as asymmetric cryptography because it uses mathematical modelling for public key encryption systems. A prime factor can be visualized by understanding Euclid's geometric position. He saw a wholenumber as a line segment, which has a smallest line segment greater than 1 that can divide equallyinto it. By the fundamental theorem of arithmetic, every positive integer has a unique primefactorization. However, the fundamental theorem of arithmetic gives no insight into how to obtain aninteger's prime factorization; it only guarantees its existence. The basic method of prime factorisation is known asthe Fermat's method. All other method is modifications of this elegant basic technique. Thefactorisation of the large semi-prime number is the key to a secure communication [13].

5. Review of Existing Approaches

This section aims to present a summary of existing articles related to secure data sharing in the Cloud. The articles presented in this section do not concentrate precisely on secure data sharing in the Cloud, rather the main necessities that will allow it. The study of secure data sharing in the Cloud is fairly novel and has turn out to be increasingly significant with the progressions and rising popularity of the Cloud in addition to the developing requirement to share data between people. We classified the existing articles in two aspects: data sharing and Cloud security. There have been some journals on security and privacy in the Cloud. Xiao and Xiao [15] recognized the five concerns of Cloud computing; confidentiality, integrity, availability, accountability, and privacy and thoroughly analyzed the threats to a piece of the concerns in addition to protection strategies.

Chen and Zhao [16] outlined the necessities for attaining privacy as well as safety in the Cloud and also concisely summarized the necessities for safe sharing of the data in the Cloud. Zhou [17] proposed a review on privacy in addition to security in the Cloud concentrating on the manner in which privacy laws must also take into concern. Cloud computing and what work could be done to avert privacy in addition to security breaches of one's private information in the Cloud. Wang et al. [18] explored issues that affect managing information security in Cloud computing. It clarified the essential security requirements for enterprises to realize the dynamics of information security in the Cloud.

Saradhy and Muralidhar [19] studied the influence of the Internet on data sharing across many different organizations like government agencies and businesses. They categorized sharing of information into data dissemination, query restriction, and matching of record. They also offered an outline for safe as well as useful sharing of information on the internet. Butler [20] defined the problems of sharing of data on the Internet that permit users to conclude particulars regarding users. It is beneficial as it increases alertness to organizations that the information they chose to share with the public can still increase privacy problems and doesn't assurance the user confidentiality. Mitchley [21] described the benefits of data sharing from a banking perspective and emphasized the privacy concerns still affecting it.

Athena et al., (2018) implemented effective methods. Specifically, elliptic curve D-H for the secret key generation and ID attribute-based encryption for enhancing data security in the cloud [22]. Kang et al., (2018) proposed a novel ID-based public auditing protocol for cloud data integrity verifying with enhanced structure, privacy-preserving, and efficient aggregation authentication. Also proved that the suggested protocol could resist forgery attack beneath the assumption that the D-H problem was hard. Moreover, the suggested protocol is already compared with further ID-based auditing protocols [23].

Santhi et al., (2018) technologically advanced an innovative security framework for improving cloud security. Initially, the CSP, data owner, and data user create the secret key for the data using implementing the DH algorithm, formerly the Third Party Auditor (TPA) authenticated the generated secret information [24]. Huang et al., (2018) suggested a secure data group sharing and dissemination scheme in the public cloud based on attribute-based and timed-release conditional ID based broadcast PRE [25].

Some of the most important necessities of secure data sharing in the Cloud are as follows. Initially, the data owner must be talented to state a user group which is permitted to view his or her information. Any member of the group must be capable of gaining access to the data anytime, wherever without the data owner's involvement. No-one, except the data owner and the group members, must achieve access to the information, including the CSP. The data owner must be capable of adding new users to the group. The data owner must also be talented to cancel access rights against any group member over his or her shared information. No group member must be permitted to cancel rights or else join new users to the group.

One minor solution for attaining secure sharing of information in the Cloud is on behalf of the data owner to encode his information previously stored into the Cloud, and later the data remain information-theoretically protected beside the Cloud provider and further malevolent users. When the data owner needs to share his information in a group, he refers the key utilized for data encryption to the individual group member. Any group member can then acquire the encoded information from the Cloud and decrypt the information with the key and later doesn't want the involvement of the data owner. However, the issue with this method is that it is computationally useless and places too much load on the data owner while allowing for factors such as user revocation.

Once the data owner cancels the accessing rights to a group member, that particular member must not have permission to access the consistent data. Meanwhile, the member

currently possesses the data access key; the data owner has to re-encrypt the data using a new key, rendering the revoked member's key unusable. Once the data is re-encrypted, he needs to distribute the innovative key to the remaining group users, and this is computationally ineffective and places too much burden on the data owner once allowing for huge group sizesthat could be more than millions of users. Therefore, this solution is impossible to be deployed in the real world for very critical data such as business, government,andrelated medical data.

Therefore, if these security concerns are not properly addressed, they will prevent cloud computing's wide-ranging applications in the future.

Attribute-based encryption is a one-to-many cryptographic primitive that offers fine-grained access control over the outsourced ciphertexts. It features a mechanism that permits access control over encoded information using access strategies and ascribed attributes amongst private keys and ciphertexts. Particularly, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) permits data owner to describe the access policy over a universe of attributes in which the user desires to possess to decode the ciphertext, by which the confidentiality and access control of data can be assured [14]. On the other hand, current solutions mostly concentrate on the way to afford secure data read for users, none of these works deliberates that several users may also write the encrypted data collaboratively in cloud computing.

6. Proposed work

6.1 Problem Statement:

One of the tremendous services that cloud computing offers is the data sharing and the data storage. Customers can outsource data in cloud without having to worry about the capacity of memory or the size of data as cloud system manages the scalability of servers needed to contain it. However, one of the predominant concerns encountered in cloud is security. As more and more sensitive data and personal information are placed in the cloud, security concerns grow up.The problem of simultaneously achieving fine-grainedness, high efficiency on the data owner's side, and standard data confidentiality of cloud data sharing remain unresolved. There is no constituency between the data synchronization and data storage.Hence there is need to improve the security mechanism of the system.The research work to be carried out will solve such security issues.

6.2 Research Objectives:

The objectives are as under:-

i) To study the existing mechanism of security of data sharing in cloud computing.

ii) To propose the effective method to enhance the security of data sharing in cloud computing.

iii) To make evaluation of the proposed method.

iv) To compare the proposed method with the existing method.

6.3 Research Methodology:

DBECC is used to examine the environmental data effectively and providing the better Unbreakable Secure Data Sharing Environment in Cloud Computing.

In this proposed method, we employ a full delegation mechanism based on DBECC, which contains a central authority and a number of independent domains. Each domain has a domain authority that requests a secret parameter from the higher level authority and generates attribute secret keys for its domain user, and the secret parameter of top level domain authority is from central authority. It reduces the workload on attribute authority and achieves lightweight key management in largescale users. A partial decryption and signing construction is proposed. The users are able to outsource most of the decryption and signing computation overhead to the CSP, which is suitable for resource-constrained mobile devices.

In our scheme, we assume the communication channels between users and cloud are assumed to be secured under existing security protocols. However, some authorized users may collude their attribute secret keys together to access data, and some fully malicious users who are allowed to access public keys, may query for attribute secret keys to decrypt data. Moreover, our scheme must satisfy the usual property of unforgeability. An adversary may try to forge a signature with a policy that his attributes do not satisfy, to outsource the re-encrypted data. So our scheme must distinguish which attributes were used to generate a signature, or any other identifying information associated with the particular signer among users satisfying a given policy.

References:-

[1] Diffie,W., & Hellman ,M (1976) .New directions in cryptography IEEE Transaction on Information Theory ,22(6),(644-654).

[2] Sarathy, R., & Muralidhar, K. (2006). Secure and useful data sharing. Decision Support Systems, 42(1), 204-220.

[3] Butler, D. (2007). Data sharing threatens privacy.

[4] Athavale , A.Y., Singh k,& Sood, S(2009) July. Design a private credentials scheme based on elliptic curve cryptography .In Computational Science ,Communication systems and Network ,2009 CICSYN"09 .First International conference on (pp 332-335).IEEE.

[5] Cavalieri, S., & Cutuli, G. (2009, November). Implementing encryption and authentication in KNX using Diffie-Hellman and AES algorithms. In *Industrial Electronics, 2009. IECON'09. 35th Annual Conference of IEEE* (pp. 2459-2464). IEEE.

[6] Arshad,R., &Ikram, N (2011) .Elliptic curve cryptography based mutual authentication scheme for session initation protocol. Multimedia tools and applications ,66(2),(165-178).

[7] Pagano, F., & Pagano, D. (2011, September). Using in-memory encrypted databases on the cloud. In *Securing Services on the Cloud (IWSSC), 2011 1st International Workshop on* (pp. 30-37). IEEE.

[8] Wang, J. S., Liu, C. H., & Lin, G. T. (2011, October). How to manage information security in cloud computing. In Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on (pp. 1405-1410). IEEE.

[9] Xiao Z, Xiao Y (2012) Security and privacy in cloud computing. IEEE Commun Surveys Tutorials 99: (pp.1–17).

[10] Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 1, pp. 647-651). IEEE.

[11] Shawish, A., & Salama, M. (2014). Cloud computing: paradigms and technologies. In *Inter-cooperative collective intelligence: Techniques and applications* (pp. 39-67). Springer, Berlin, Heidelberg.

[12] Liu, H.,& Liu .Y (2014).Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic eliptic curve. Optics and Laser Technology ,56(15-19).

[13] Swathi, T., Srikanth, K., & Reddy, S. R. (2014). Virtualization in cloud computing. *International Journal of Computer Science and Mobile Computing*, *3*(5),(pp 540-546).

[14] Arockiam "Efficient Cloud Storage Confidentiality to Ensure Data Security " CCSW 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, IEEE

[15] Huang, Q., Yang, Y., & Shen, M. (2016). Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing. Future Generation Computer Systems, 72, 239–249.

[16] Cui, H., Wan, Z., Deng, R. H., Wang, G., & Li, Y. (2016). Efficient and expressive keyword search over encrypted data in cloud. IEEE Transactions on Dependable and Secure Computing, 15(3), 409-422.

[17] Athena, J., Sumathy, V., & Kumar, K. (2017). An identity attribute-based encryption using elliptic curve digital signature for patient health record maintenance. International Journal of Communication Systems, 31(2), 34-39.

18] Shaikh, A., Pathan, R., Patel, R., & Rukaiya, A. P. S. (2018). Implementation of Authentication using Graphical Password for Cloud Computing. International Research Journal of Engineering and Technology, 5(5), 3293-3297.

[19] Zhang, Y., He, D., & Choo, K. K. R. (2018). BaDS: Block-chain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT. Wireless Communications and Mobile Computing, 2018.

[20] Kang, B., Si, L., Jiang, H., Li, C., & Xie, M. (2018). ID-Based Public Auditing Protocol for Cloud Data Integrity Checking with Privacy-Preserving and Effective Aggregation Verification. Security and Communication Networks, 2018.

[21]Shen, J., Zhou, T., Chen, X., Li, J., & Susilo, W. (2018). Anonymous and traceable group data sharing in cloud computing. IEEE Transactions on Information Forensics and Security, 13(4), 912-925